CUBIC CONGRUENCES WITH THREE REAL ROOTS

By Edward B. Escott

Gauss has shown that the complete solution of the equation

$$x^n_a - 1 = 0$$

where n is prime, is found by solving some auxiliary equations whose degrees are the factors of $n - 1$. These equations are called cyclotomic equations. Gauss showed that these equations are irreducible.

Consider, for example, the equation

$$x^7 - 1 = 0. \tag{1}$$

Calling one of its complex roots ω, the remaining roots are ω^2, ω^3, ω^4, ω^5, ω^6, $\omega^7 = 1$.

Since the sum of the roots of (1) is zero, we have

$$1 + \omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6 = 0. \tag{2}$$

Arrange the roots so that the exponents are in geometrical progression. Several groupings are possible:

$$\begin{array}{l} \omega,\ \omega^2,\ \omega^4,\ \omega^8\ (= \omega),\ \cdots \\ \omega^3,\ \omega^6,\ \omega^{12}\ (= \omega^5),\ \omega^{24}\ (= \omega^3),\ \cdots \end{array} \tag{3}$$

i. e., two groups of three each; or

$$\begin{array}{l} \omega,\ \omega^6,\ \omega^{36}\ (= \omega),\ \cdots \\ \omega^2,\ \omega^{12}\ (= \omega^5),\ \omega^{72}\ (= \omega^2),\ \cdots \\ \omega^3,\ \omega^{18}\ (= \omega^4),\ \omega^{108}\ (= \omega^3),\ \cdots \end{array} \tag{4}$$

i. e., three groups of two each.

If we take the sum of the roots in the same row in (3) for roots of a new equation, i. e.

$$a = \omega + \omega^2 + \omega^4, \qquad \beta = \omega^3 + \omega^6 + \omega^5, \tag{5}$$

we shall have

$$x^2 + x + 2 = 0 \tag{6}$$

with the roots a and β.

Similarly, in (4) if we put

$$a = \omega + \omega^6, \qquad \beta = \omega^2 + \omega^5, \qquad \gamma = \omega^3 + \omega^4, \tag{7}$$

the equation whose roots are a, β, γ is

$$x^3 + x^2 - 2x - 1 = 0. \tag{8}$$

Equations (6) and (8) are the cyclotomic equations for the division of the circle into seven parts.*

From (7), $a^2 = \omega^2 + 2\omega^7 + \omega^{12} = \omega^2 + 2 + \omega^5 = \beta + 2$; also $\beta^2 = \gamma + 2$, and $\gamma^2 = a + 2$.

From these relations, we see that all the roots of (8) can be obtained from any one root, and since (8) must have one real root, all of its roots must be real.

In order to apply these results to cubic congruences with modulus an odd prime, let us summarize briefly a few of the properties of these congruences.

A congruence cannot have more roots than its degree. The degree of a congruence (mod p) can always be reduced to $p - 2$ by Fermat's Theorem.

$$x^{p-1} \equiv 1 \pmod{p}, \qquad x \not\equiv 0 \pmod{p}.$$

A congruence of the first degree always has a root.

A congruence of the second degree has two roots or none.

A congruence of the third degree has (a) three roots, (b) one root, or (c) no roots.

The condition that a cubic congruence shall have three roots is rather involved, so it seems of interest to consider a large class of congruences which have three roots (when they have one).

An example is obtained at once from (8).

If the congruence

$$x^3 + x^2 - 2x - 1 \equiv 0 \pmod{p} \tag{9}$$

has a root a, it is evident that it has also the roots $\beta = a^2 - 2$ and $\gamma = \beta^2 - 2$.

* For details see Mathews' *Theory of Numbers.*

Let us consider the problem, to find the most general irreducible cubic equation in which each root is a rational integral function of another root, i. e.,

$$\beta = f(\alpha), \qquad \gamma = f(\beta), \qquad \alpha = f(\gamma),$$

and let the equation whose roots are α, β, γ be

$$x^3 + ax^2 + bx + c = 0; \tag{10}$$

then by using the relation

$$\alpha^3 + a\alpha^2 + b\alpha + c = 0$$

and similar ones for β and γ, we can replace $f(\alpha)$ by a function of the second degree.

Consider first the case where the roots have the relations

$$\beta = \alpha^2 - n, \qquad \gamma = \beta^2 - n, \qquad \alpha = \gamma^2 - n, \tag{11}$$

and let α, β, γ be roots of (10).

Form the equation whose roots are the squares of the roots of the given equation, by transposing the terms of even degree to the second member, squaring both members, and replacing x^2 by x. We have

$$x^3 + (2b - a_2)\, x^2 + (b^2 - 2ac)\, x - c^2 = 0. \tag{12}$$

If we increase the roots of the given equation (10) by n, we shall have

$$x^3 + (-3n + a)\, x^2 + (3n^2 - 2an + b)\, x + (-n^3 + an^2 - bn + c) = 0. \tag{13}$$

These two equations must be identical. Equating coefficients,

$$2b - a^2 = -3n + a, \tag{14}$$

$$b^2 - 2ac = 3n^2 - 2an + b, \tag{15}$$

$$c^2 = n^3 - an^2 + bn - c. \tag{16}$$

From (14)

$$n = \tfrac{1}{3}\,(a^2 + a - 2b). \tag{17}$$

Substituting in (15) and solving for c,

$$c = -\frac{1}{6a}\,(a^4 - 4a^2b - a^2 + b^2 + 3b). \tag{18}$$

Substituting these values of n and c in (16) and arranging with reference to b, we have

$$\begin{aligned} &3b^4 + (8a^2 + 18)\, b^3 + (6a^4 - 6a^2 - 18a + 27)\, b^2 \\ &- (18a^4 - 36a^3 + 18a^2 + 54a)\, b - (a^8 - 6a^6 + 10a^5 - 3a^4 - 18a^3) = 0. \end{aligned} \tag{19}$$

We can tell some of the roots of (19) at once. For example, in (11) if $\gamma = \beta = \alpha$, we have $n = \alpha^2 - \alpha$; and since (10) becomes $(x - \alpha)^3 = 0$, we have $\alpha = -a/3$; whence $n = (a^2 + 3a)/9$ and from (14)

$$b = \frac{a^2}{3}. \tag{20}$$

This is one root of (19).

In (11) instead of α, β, and γ being different, one root might be repeated. Instead of (11) we would have

$$\alpha = \alpha^2 - n, \qquad \beta = \beta^2 - n, \qquad (\beta \neq \alpha). \tag{21}$$

Subtracting, $\alpha - \beta = \alpha^2 - \beta^2$, i. e., $1 = \alpha + \beta$, whence $\beta = -\alpha + 1$.

Equation (10) becomes

$$(x + \alpha)^2\,(x + \alpha - 1) = 0, \tag{22}$$

and comparing coefficients with (10) we find $a = -\alpha - 1$, $b = -\alpha^2 + 2\alpha$, whence $\alpha = -a - 1$, and

$$b = -(a^2 + 4a + 3). \tag{23}$$

This gives another root of (19).

In place of (11) if we had taken the relations

$$\alpha = \alpha^2 - n, \qquad \beta = \gamma^2 - n, \qquad \gamma = \beta^2 - n \tag{24}$$

we would have the same equations (14), (15), and (16). From the last two equations $\beta - \gamma = \gamma^2 - \beta^2$, and since $\beta \neq \gamma$, $1 = -\gamma - \beta$, i. e., $\gamma = -\beta - 1$. Substituting in the second or third relation of (24), we have

$$\beta^2 + \beta - n + 1 = 0. \tag{25}$$

Therefore, α, β, γ are roots of the equation

$$(x - \alpha)(x^2 + x - n + 1) = 0. \tag{26}$$

Equating coefficients of (26) and (10), we find $-\alpha + 1 = a$, and $-\alpha - n + 1 = b$, whence $\alpha = -a + 1$; and since $n = \alpha^2 - \alpha = a^2 - a$, we have

$$b = -(a^2 - 2a). \tag{27}$$

This gives a third root of (19).

Therefore, the remaining root of (19), and the only one which gives for (10) an irreducible equation, is

$$b = -(a^2 - 2a + 3). \tag{28}$$

From (17) and (18) we have, with this value of b,

$$c = -(a^3 - 2a^2 + 3a - 1),$$

$$n = a^2 - a + 2.$$

Then the equation

$$x^3 + ax^2 - (a \quad - 2a + 3)\, x - (a \quad - 2a^2 + 3a - 1) = 0 \tag{29}$$

has its roots α, β, γ connected by the relations

$$\begin{aligned} \beta &= \alpha^2 - (a^2 - a + 2), \\ \gamma &= \beta^2 - (a^2 - a + 2), \\ \alpha &= \gamma^2 - (a^2 - a + 2), \end{aligned} \tag{30}$$

and since it has one real root, all its roots are real.

The application to cubic congruences is immediate. We have the theorem:

The congruence

$$x^3 + ax^2 - (a^2 - 2a + 3)\, x - (a^3 - 2a^2 + 3a - 1) \equiv 0 \pmod{p}$$

has three roots (when it has any), the relations between the roots being given in equations (30).*

* We will have the same relations (30) between the roots if we replace a by $-(a - 1)$ This gives two irreducible cubic congruences having the same relations between their roots.

To find irreducible cubic equations or congruences, having between their roots a more general relation than (11), namely

$$\begin{aligned} \beta &= \alpha^2 + k\alpha + l, \\ \gamma &= \beta^2 + k\beta + l, \\ \alpha &= \gamma^2 + k\gamma + l, \end{aligned} \tag{31}$$

we could use the preceding method, or we can obtain the results from those already obtained, as follows:

Equations (31) may be written,

$$\begin{aligned} \beta + \frac{k}{2} &= \left(\alpha + \frac{k}{2}\right)^2 - \frac{k^2 - 2k - 4l}{4}, \\ \gamma + \frac{k}{2} &= \left(\beta + \frac{k}{2}\right) - \frac{k^2 - 2k - 4l}{4}, \\ \alpha + \frac{k}{2} &= \left(\gamma + \frac{k}{2}\right) - \frac{k^2 - 2k - 4l}{4}. \end{aligned} \tag{32}$$

Increase the roots of (10) by $k/2$, and we have

$$x^3 + \left(a - \frac{3k}{2}\right)x^2 + \left(b - ak + \frac{3k^2}{4}\right)x + \left(c - \frac{bk}{2} + \frac{ak^2}{4} - \frac{k^3}{8}\right) = 0. \tag{33}$$

Substitute in the results previously found the coefficients of (33) in place of a, b, and c, and $(k^2 - 2k - 4l)/4$ in place of n; we have, then:—

The congruence

$$x^3 + ax^2 + bx + c \equiv 0 \pmod{p}$$

has three roots (when it has any), the relations between he roots being

$$\begin{aligned} \beta &= \alpha^2 + k\alpha + l, \\ \gamma &= \beta^2 + k\beta + l, \\ \alpha &= \gamma^2 + k\gamma + l, \end{aligned}$$

where

$$\begin{aligned} b &= -\,(a^2 - 4ak - 2a + 3k^2 + 3k + 3), \\ c &= -\,(a^3 - 4a^2k - 2a^2 + 5ak^2 + 5ak + 3a - 2k^3 - 3k^2 - 3k - 1), \\ l &= -\,(a^2 - 3ak - a + 2k^2 + 2k + 2).^* \end{aligned}$$

* We will have the same relations between the roots if we replace a by $-a + 3k + 1$. This gives two irreducible cubic congruences having the same relations between the roots.

Finally, the equation whose roots have the most general relation of the second degree,

$$\begin{aligned} \beta &= f\alpha^2 + g\alpha + h, \\ \gamma &= f\beta^2 + g\beta + h, \\ \alpha &= f\gamma^2 + g\gamma + h, \end{aligned} \tag{34}$$

can easily be found from the preceding. Equation (34) may be written in the form

$$\begin{aligned} f\beta &= (f\alpha)^2 + g(f\alpha) + fh, \\ f\gamma &= (f\beta)^2 + g(f\beta) + fh, \\ f\alpha &= (f\gamma)^2 + g(f\gamma) + fh, \end{aligned} \tag{35}$$

which is like (31) with $f\alpha$, $f\beta$, $f\gamma$ in place of α, β, γ; g in place of k; and fh in place of l.

If α, β, γ are roots of

$$x^3 + ax^2 + bx + c = 0,$$

$f\alpha$, $f\beta$, $f\gamma$ are roots of

$$x^3 + afx^2 + bf^2x + cf^3 = 0.$$

The corresponding theorem is:

The congruence

$$x^3 + ax^2 + bx + c \equiv 0 \qquad (\mathrm{mod}\ p)$$

has three roots (when it has any), the relation between the roots being

$$\begin{aligned} \beta &= f\alpha^2 + g\alpha + h, \\ \gamma &= f\beta^2 + g\beta + h, \\ \alpha &= f\gamma^2 + g\gamma + h, \end{aligned}$$

where

$$\begin{aligned} bf^2 &= -(a^2f^2 - 4afg - 2af + 3g^2 + 3g + 3), \\ cf^3 &= -(a^3f^3 - 4a^2f^2g - 2a^2f^2 + 5afg^2 + 5afg + 3af - 2g^3 - 3g^2 - 3g - 1), \\ hf &= -(a^2f^2 - 3afg - af + 2g^2 + 2g + 2). \end{aligned}$$

UNIVERSITY OF MICHIGAN
ANN ARBOR.